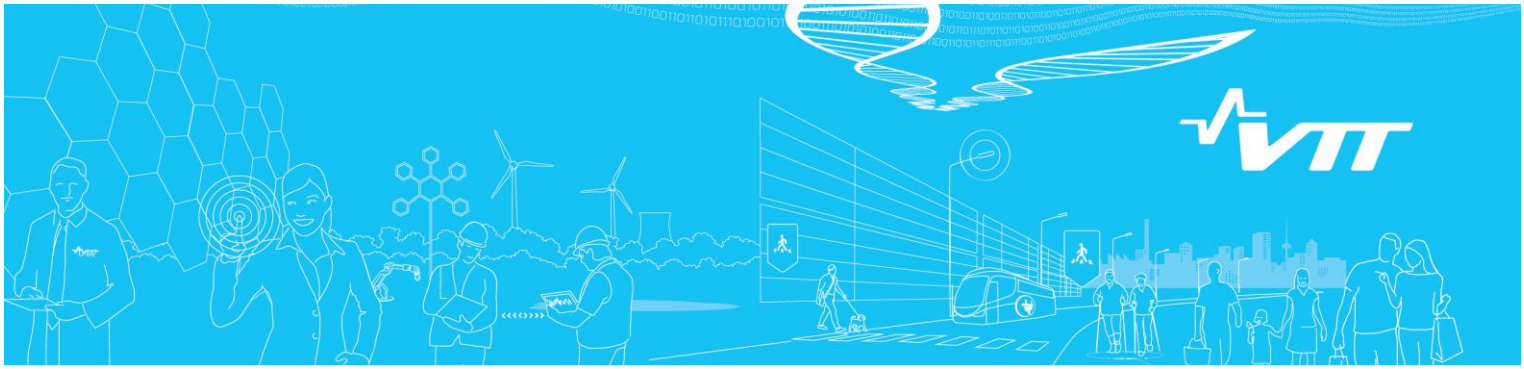
VTT Technical Research Centre of Finland

Probabilistic risk model of digital reactor protection system

Tyrväinen, Tero; Porthin, Markus

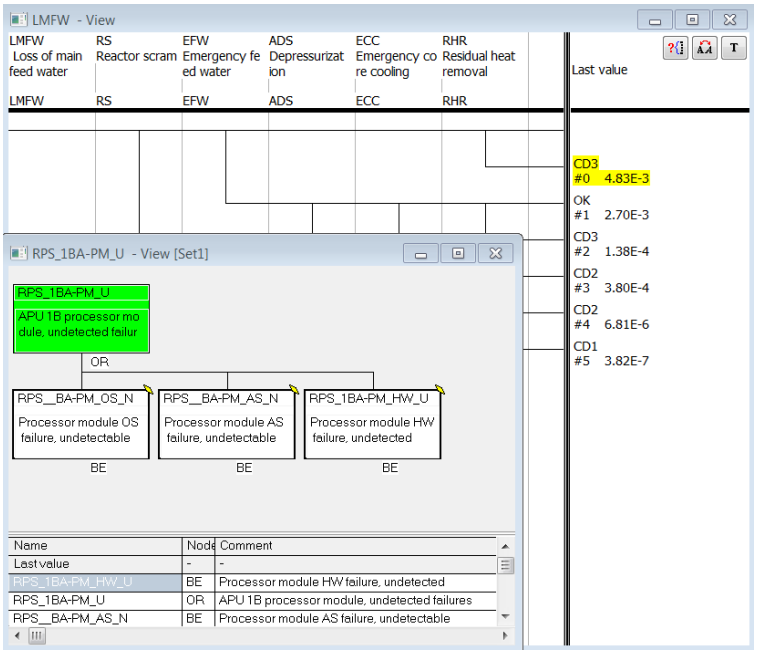
Published: 01/01/2018

Document Version
Publisher's final version



RESEARCH REPORT

VTT-R-06631-18



Probabilistic risk model of digital reactor protection system

Authors: Tero Tyrväinen, Markus Porthin

Confidentiality: Public

Report's title Probabilistic risk model of digital reactor protection system	
Customer, contact person, address VYR	**Order reference** SAFIR 5/2018
Project name Integrated safety assessment and justification of nuclear power plant automation	**Project number/Short name** 117229/SAUNA
Author(s) Tero Tyrväinen, Markus Porthin	**Pages** 27/
Keywords Probabilistic risk assessment, digital I&C, software reliability	**Report identification code** VTT-R-06631-18

Summary

This report presents a probabilistic risk assessment (PRA) model of a nuclear power plant focusing on digital I&C in the reactor protection system (RPS). The model is prepared for an international benchmark study in WGRISK project DIGMAP. The model contains one event tree representing loss of main feed-water accident in a fictive boiling water reactor plant. The model is very simplified. Only the RPS is modelled in detailed, because that is the focus of the benchmark study.

The selected modelling approach is close to the previous model of the DIGREL project employing small fault trees as building blocks. I&C component failures have been divided into detected failures and undetected failures. Significant portion of the contribution of the RPS related risk comes from application software failures, along with undetected hardware failures. On the other hand, detected hardware failures in the RPS have insignificant contribution to the core damage risk, likely because spurious actuations have not been analysed. The importance of automatic testing and periodic testing as fault tolerant techniques to reduce the risk of undetected hardware failures was recognized in the sensitivity studies. Selection of common cause failure groups and parameters, and application software basic events are expected to be major issues in the benchmark study.

Confidentiality	Public

Espoo, 9.1.2019

Written by	**Reviewed by**	**Accepted by**
Tero Tyrväinen, Research scientist	Kim Björkman, Research scientist	Juha Kortelainen, Research team leader

VTT's contact address
VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND

Distribution (customer and VTT)
SAFIR2018 RG1 members, VTT archive, DIGMAP project group

Contents

List of acronyms

Acronym	Meaning
AC	Air cooler
ADS	Automatic depressurisation system
AI	Analog input
APU	Acquisition and processing unit
AS	Application software
BWR	Boiling water reactor
CCF	Common cause failure
CCW	Component cooling water system
CD	Core damage
CL	Communication link
CP	Condensation pool
CV	Check valve
DI&C	Digital instrumentation and control
DO	Digital output
DWST	Demineralized water storage tank
ECC	Emergency core cooling system
EFW	Emergency feed-water system
ESF	Engineered safety features
HVA	Heating, venting and air conditioning system
HW	Hardware
HX	Heat exchanger
I&C	Instrumentation and control
IDN	Inter-division network
LMFW	Loss of main feed-water
MFW	Main feed-water system
MP	Motor-operated pump
MV	Motor-operated valve

NEA	Nuclear energy agency
NPP	Nuclear power plant
OECD	Organisation for economic co-operation and development
OS	Operating system
PM	Processor module
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
PTU	Periodic testing unit
RCO	Reactor containment
RHR	Residual heat removal system
RPS	Reactor protection system
RPV	Reactor pressure vessel
RS	Reactor scram system
SL	Sensor measuring water level
SP	Sensor measuring pressure
SR	Sub-rack
ST	Sensor measuring temperature
SWS	Service water system
VU	Voting unit
WDT	Watchdog timer
WGRISK	Working group on risk assessment

1. Introduction

In 2015, the OECD Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRISK) completed a study on failure mode taxonomy for reliability assessment of digital instrumentation and control (DI&C) systems for probabilistic risk assessment (PRA) [1]. The report provides a good taxonomy framework for reliability modelling of DI&C. However, there is still a lack of consensus on an appropriate modelling approach for the purpose of PRA. Therefore, a three-year WGRISK task *Digital I&C PSA – Comparative application of DIGital I&C Modeling Approaches for PSA (DIGMAP)* was started in 2017 [2].

The objective of DIGMAP is to compare modelling approaches for safety-important DI&C systems in an example nuclear power plant (NPP) for the purpose of PRA. Through the comparison, various approaches and valuable insights concerning e.g. methods, used level of detail and quantification issues for future modelling method development can be identified. For the benchmark study, a common example plant description [3] has been developed based on the DIGREL PRA model [4]. The plant is a fictive boiling water reactor (BWR) plant with simplified systems except for the more detailed digital I&C reactor protection system. One example accident case is considered (loss of main feed-water, LMFW). Each participant is expected to develop its own PRA model based on the provided system layout of the example NPP. The different models will be shared, discussed and compared. This report presents the VTT's model to be used in the benchmark study.

2. Plant and reactor protection system description

The plant is a generic and simplified BWR plant. The layout of main safety systems is presented in Figure 1, and the safety systems are also listed in Table 1. Each safety system, except for the reactor protection system, contains only one train.

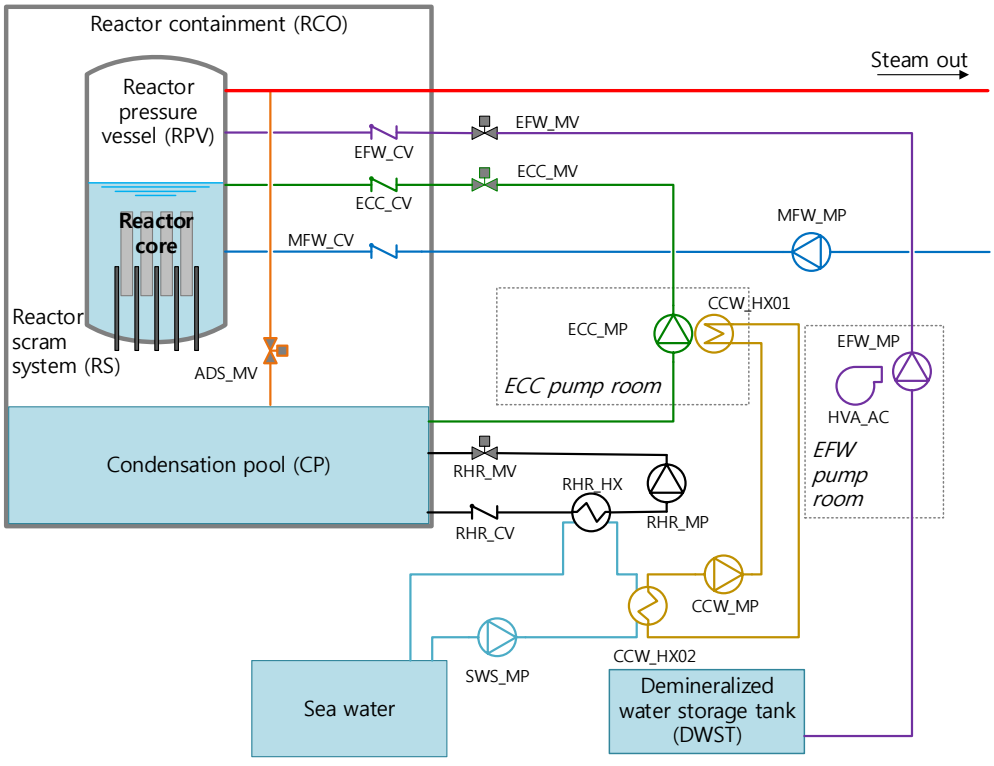


Figure 1: The layout of main safety systems [3].

Table 1: Safety systems.

System	Acronym
Automatic depressurization system	ADS
Component cooling water system	CCW
Emergency core cooling system	ECC
Emergency feed-water system	EFW
Service water system	SWS
Heating, venting and air conditioning system	HVA
Main feed-water system	MFW
Residual heat removal system	RHR
Reactor scram system	RS

The reactor protection system (RPS) consists of two diverse subsystems, RPS-A and RPS-B. Both subsystems contain four divisions. Each division contains its own measurement sensors, acquisition and processing unit (APU), voting unit (VU) and sub-rack (SR). Each unit contains a processor module (PM) and a communication link (CL) module. Each APU contains analog input (AI) modules receiving signals from measurement sensors, and each VU contains a digital output (DO) module sending signals to the actuators. In the PM of each VU, 2-out-of-4 voting is performed based on inputs from the APUs of all division. The layout of the reactor protection system is presented in Figure 2. A safety function is actuated if any of the divisions sends it an actuation signal. The actuation signals of components are summarised in Table 2.

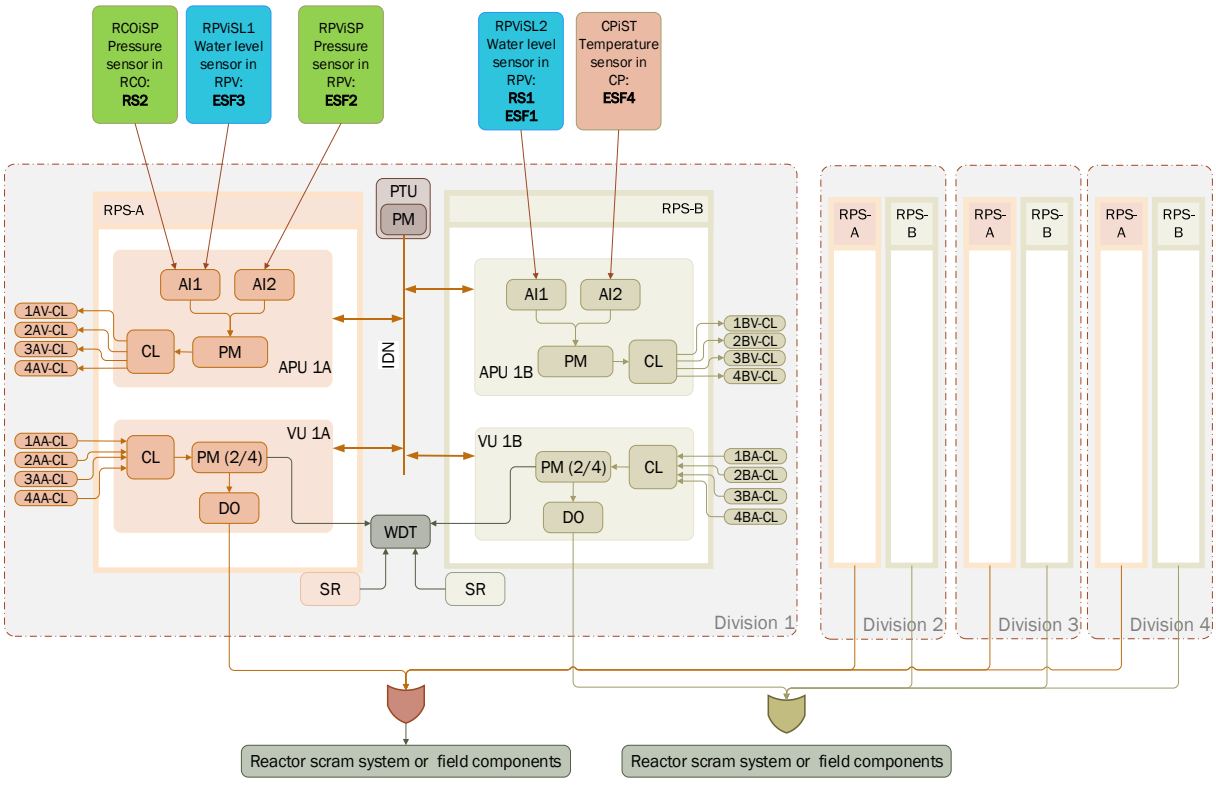


Figure 2: Reactor protection system layout [3].

Table 2: Actuation signals [3].

System	Component	Control	Conditions	Signal
RS	Control rods	Open	RS1: low water level in reactor RS2: high pressure in containment	RS1 + RS2
EFW	Pump	Start	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
	Motor-operated valve	Open	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
HVA	AC cooler	Start	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
ADS	Pressure relief valve	Open	ESF2: high pressure in reactor	ESF2
ECC	Pump	Start	ESF3: low water level in reactor	ESF3
	Motor-operated valve	Open	ESF3: low water level in reactor	ESF3
RHR	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
	Motor-operated valve	Open	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
CCW	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
SWS	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4

The 2-out-of-4 voting logic is degraded to 2-out-of-3 if a failure is detected in one of the inputs. After two detected failures, the voting logic is 1-out-of-2. If three failures are detected, actuation is performed. Spurious actuation is however out of the scope of the study.

Each division contains a periodic testing unit (PTU) that is common to both subsystems. Some of the I&C hardware (HW) failures can be detected by the periodic testing that is performed every 24 hours. The PTU gathers the information from I&C components through inter-division network (IDN). Each division also contains a watchdog timer (WDT) that is common to both subsystems. The WDT can detect some of the HW failures in the PMs of the VUs and SRs in real time.

Each processor module consists of HW, operating system (OS) and application software (AS). Other I&C modules consist of HW and OS. The model description [3] contains fictive failure data of HW, OS and AS of each module. OS and AS failure probabilities are defined on demand basis, and they are assumed to be always undetected. For HW failures, failure rate is given and it is divided for failures detected by different fault tolerant features, which are automatic testing, periodic testing and full-scope testing. All HW failures are detected by full-scope testing performed every half a year if they are not detected earlier by other features.

The model description [3] also provides failure data of mechanical components and common cause failure parameters to be used in the models.

3. Event tree

Loss of main feed-water is the only accident scenario analysed in the benchmark study. The event tree is presented in Figure 3 and it is also given in the model description [3] to the participants of the benchmark study.

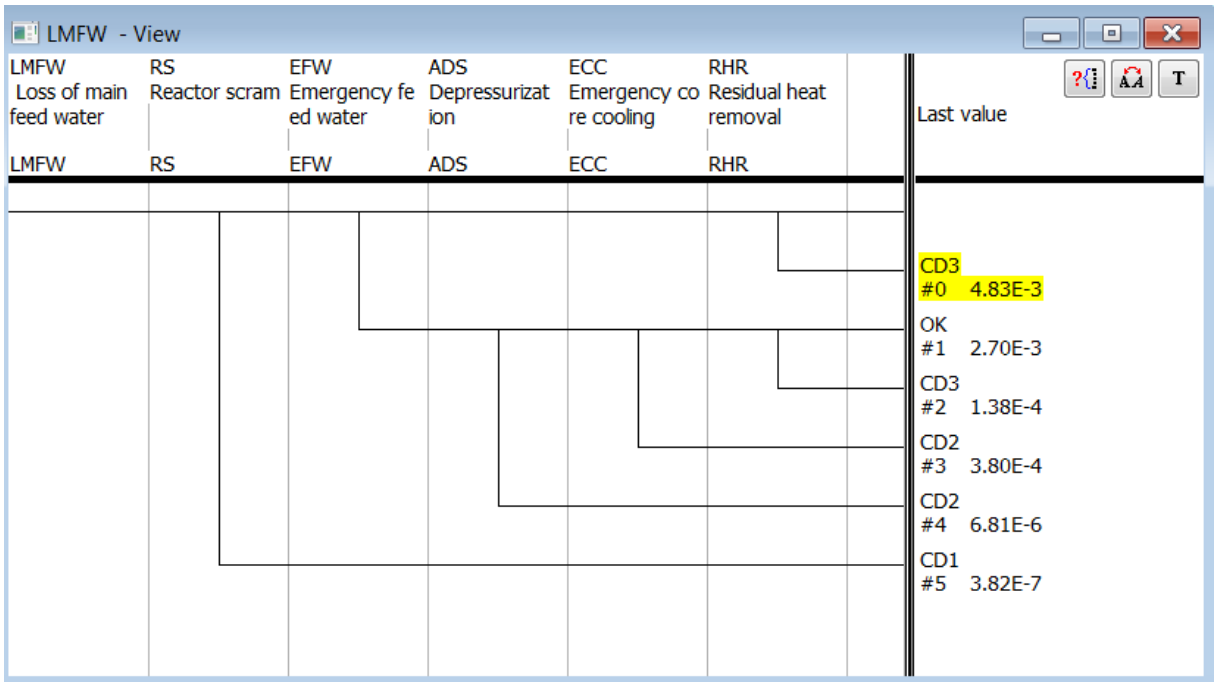


Figure 3: Event tree for loss of main feed-water accident.

4. Basic events

Basic events of mechanical components are not presented here. They are given in Table 3 of the model description [3]. In addition, two basic events are assigned to each measurement sensor representing detected and undetected failure. All failures are assumed to be detected by full-scope testing. The undetected failure represents the unavailability related to the time before the detection when the failure is latent. Respectively, the detected failure represents the unavailability related to the time after detection but before repair. The probability of an undetected failure is the probability that a failure occurs and after the failure a demand occurs before the full-scope testing (performed every half a year). It is calculated as

$$P_u = 1 - \frac{1}{\lambda T_t}\left(1 - e^{-\lambda T_t}\right), \quad (1)$$

where λ is the failure rate (2.0E-7/h for sensors [3]), and T_t is the testing interval (4380 hours for full-scope testing). Therefore, the probability of an undetected failure is 4.38E-4 for each sensor. The probability of a detected failure is the probability that a failure occurs and a demand occurs after detection before the component has been repaired. It is calculated as

$$P_d = \lambda T_r, \quad (2)$$

where T_r is the mean time to repair (8 hours for all components). Therefore, the probability of a detected failure is 1.60E-6 for each sensor.

For an RPS module, there are two HW basic events, detected and undetected failure. The probability of the detected failure is calculated by equation (2). The total failure rate (given in [3]) is used in the computation because all failures are always detected sooner or later, and the mean time to repair is the same regardless of the detection mechanism. The time that a failure is latent is included in the probability of the undetected failure. The probability of the undetected failure is more complicated to calculate because of various fault tolerant features. It is discussed separately in Section 5.1.

OS and AS basic events are common to all divisions, which means that a common cause failure (CCF) between all divisions is assumed if one module fails. The failure probabilities are given directly in the model description [3]. For each module, there is one OS basic event. For each processor module, there is one AS basic event, which means that AS is not divided into smaller parts according to signals that are processed. The basic event represents the failure of all signal processing in the module.

All RPS basic event types and their probabilities are presented in Table 3. All HW basic events represent failure of one specific module in a single division only, whereas OS and AS basic events represent common cause failure between modules in all divisions.

Table 3: RPS basic events.

Module	Type of failure	Probability
APU AI	Undetected HW failure	8.87E-4
APU AI	Detected HW failure	1.60E-5
APU AI	OS failure	1.00E-5
APU PM	Undetected HW failure	4.52E-4
APU PM	Detected HW failure	1.60E-5
APU PM	OS failure	1.00E-5
APU PM	AS failure	1.00E-4
APU CL	Undetected HW failure	2.29E-3
APU CL	Detected HW failure	4.00E-5
APU CL	OS failure	1.00E-5
VU DO	Undetected HW failure	9.17E-4
VU DO	Detected HW failure	1.60E-5
VU DO	OS failure	1.00E-5
VU PM	Undetected HW failure	4.45E-4
VU PM	Detected HW failure	1.60E-5
VU PM	OS failure	1.00E-5
VU PM	AS failure	1.00E-4
VU CL	Undetected HW failure	2.29E-3
VU CL	Detected HW failure	4.00E-5
VU CL	OS failure	1.00E-5
SR	Undetected HW failure	7.30E-6
SR	Detected HW failure	1.60E-5
SR	OS failure	1.00E-5

PTU or WDT failures have not been included in the model explicitly. Scenarios related to them are included in the probabilities of undetected HW failures as described in Section 5.1.

5. Challenging issues

5.1 Probabilities of undetected HW failures

The failure data of HW failures is divided according to fault tolerant features [3] as presented in Table 4. In the table, F refers to full-scope testing, A refers to automatic testing and P refers to periodic testing. The failure rates are divided for different fault tolerant techniques according to the fractions given in the table. Some failures can be detected by two or three fault tolerant techniques. It is assumed that all HW failures are detected in full-scope testing if they are not detected by other means. For example, 60% (P(AF)+P(APF) = 0.4+0.2) of HW failures of an APU AI module are detected primarily by automatic testing (performed by the PM of the APU) and 20% primarily by periodic testing (performed by PTU). Failures that can be detected both by automatic testing and periodic testing (APF) are primarily detected by automatic testing because it is performed in real time. If automatic testing fails, one third (0.2/0.6) of failures that would have been detected by automatic testing are detected by periodic testing.

Table 4: RPS hardware failure data [3].

Module	Failure rate (/h)	F	AF	PF	APF
APU AI	2E-6	0.2	0.4	0.2	0.2
APU PM	2E-6	0.1	0.7	0.1	0.1
APU CL	5E-6	0.2		0.8	
VU DO	2E-6	0.2		0.8	
VU PM	2E-6	0.1	0.7	0.1	0.1
VU CL	5E-6	0.2		0.8	
PTU PM	2E-6	1			
PTU IDN	1E-6	0.8		0.2	
SR	2E-6		0.9	0.1	

A basic event representing an undetected failure combines all failures not detected by automatic testing. These failures can be classified as follows:

1. Failures that are detected by full-scope testing only
2. Failures that are primarily detected by periodic testing
    a. Failures detected by periodic testing

   b. Failures detected by full-scope testing because of a failure of a component needed in periodic testing

3. Failures that are not detected by automatic testing because of a failure of a component needed in automatic testing

   a. Failures detected by periodic testing

   b. Failures that cannot be detected by periodic testing and are detected by full-scope testing

   c. Failures detected by full-scope testing because of a failure of a component needed in periodic testing.

The basic event represents the unavailability before detection (all HW failures are detected eventually). A supporting fault tree (not appearing in the actual model) is used to calculate the probability of the basic event.

The supporting fault tree of an undetected APU CL failure is presented in Figure 4. In it, basic event APUCL_F represents failures detected by full-scope testing only (case 1 above), and basic event APUCL_P represents failures detected primarily by periodic testing (case 2a above). The probabilities of these basic events are calculated according to equation (1) so that the failure rate is not the total failure rate, but the failure rate related to the detection mechanism ($0.8 \cdot 5.0 \cdot 10^{-6} = 4.0 \cdot 10^{-6}$ for failures detected by periodic testing, and $0.2 \cdot 5.0 \cdot 10^{-6} = 1.0 \cdot 10^{-6}$ for failures detected by full-scope testing). The testing interval is 24 hours for periodic testing and half a year for full-scope testing. The AND gate in the fault tree is related to scenarios where periodic testing fails, and the failures can only be detected by full-scope testing (case 2b above). Basic event APUCL_PF represents failures that would have normally been detected by periodic testing, but are detected by full-scope testing in this scenario. There are six basic events causing the failure of periodic testing in the PTU:

- PTUPM_F: HW failure of the PM in the PTU,
- PTUIDN_F: HW failure of the IDN detected by full-scope testing,
- PTUIDN_P: HW failure of the IDN detected by periodic testing,
- PTUPMOS_N: OS failure of the PM in the PTU,
- PTUPMAS_N: AS failure of the PM in the PTU,
- PTUIDNOS_N: OS failure of the IDN.

The probability of APUCL_PF has been calculated according to equation (1). The testing interval is half a year. Basic events PTUPM_F, PTUIDN_F and PTUIDN_P represent unavailability before and after detection. It is assumed that the detection of a PTU failure does not affect the functioning of the RPS, e.g. change the voting logic. Therefore, the probabilities of the basic events are sum values of values calculated using equations (1) and (2).

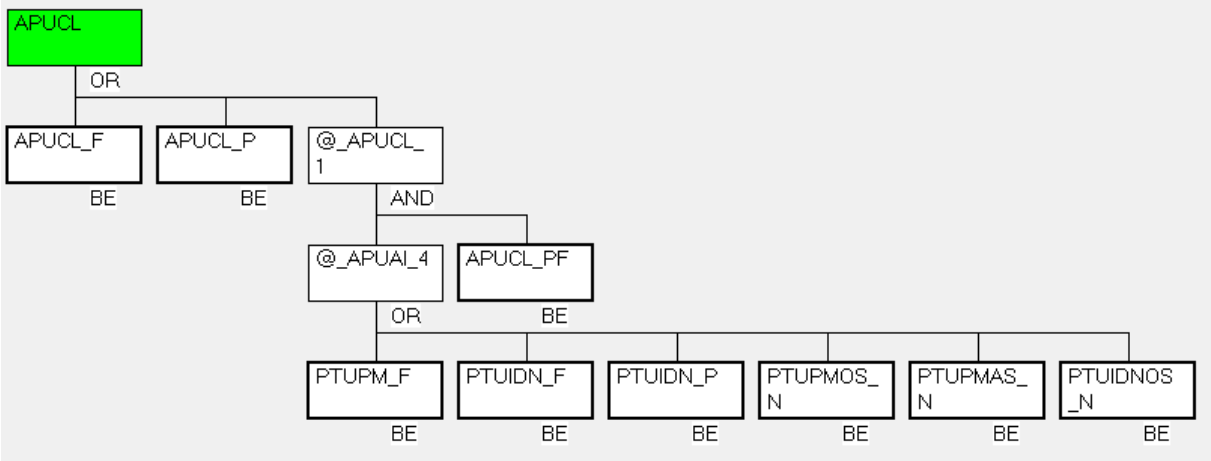


Figure 4: Fault tree of undetected APU CL failure.

The fault tree produces the following minimal cut sets:

S1-sum 2.29E-03

Num	Prob.	%	Cumul	Prob	Name
1	2.19E-03	95.53	95.53	2.19E-03	APUCL_F
2	4.80E-05	2.10	97.62	4.80E-05	APUCL_P
3	3.82E-05	1.67	99.29	8.71E-03 4.38E-03	APUCL_PF PTUPM_F
4	1.53E-05	0.67	99.96	8.71E-03 1.76E-03	APUCL_PF PTUIDN_F
5	8.71E-07	0.04	100.00	8.71E-03 1.00E-04	APUCL_PF PTUPMAS_N
6	8.71E-08	0.00	100.00	8.71E-03 1.00E-05	APUCL_PF PTUIDNOS_N
7	8.71E-08	0.00	100.01	8.71E-03 1.00E-05	APUCL_PF PTUPMOS_N
8	3.48E-08	0.00	100.01	8.71E-03 4.00E-06	APUCL_PF PTUIDN_P

The total probability 2.29E-3 is used in the actual model. It is conservative to multiply the probability of APUCL_PF directly with the probabilities of PTUPM_F, PTUIDN_F and PTUIDN_P, because a PTU failure needs to occur before APUCL_PF so that the CL failure is not detected, but this formula just multiplies the unavailabilities. In addition, PTUIDN_P is detected in 24 hours. A more accurate way to perform the calculations could be found, but it would require information about test times, such as the difference between the full-scope test times of the CL and PTU. The approximation obtained by multiplying unavailabilities is considered sufficient, because the CL failure probability is dominated by APUCL_F, and this fault tree analysis can already be considered quite a heavy procedure compared to the significance of the PTU failure scenarios.

The CL failure analysis was presented above, because it is the simplest analysis scenario, along with identical digital output module case. Analysis of processor modules and sub-racks is more complicated, because also the failure of automatic testing needs to be included in the analysis. In the case of an analog input module, scenarios related to the failures of automatic testing performed by the APU PM are not included, because the failure of the APU PM itself has the same effect as the failure of AI module, and the scenarios are thus covered by PM basic events. The analyses are not presented here, but the principles are the same as in the CL case. SR is the only case where failures of fault tolerant techniques contribute significantly to the probability of an undetected failure, because all failures are detected either by automatic testing or periodic testing when the WDT and PTU are working. Because of the same reason, the failure probability of a SR is also quite small.

The approach to calculate probabilities of undetected failures is quite similar to the approach presented in [5]. However, in [5], failures of fault-tolerant techniques were not considered, only the fault coverages of different techniques.

5.2 Common cause failures

Each RPS HW basic event belongs to an alpha factor CCF group of four components, one component coming from each division. The CCF parameters are taken from the model description [3]. For detected failures, parameters α_3 and α_4 are however set to 0, because three detected failures are assumed to cause the actuation of a safety function, which means that CCFs with three or four modules cannot contribute to the failure of the safety function.

The software basic events are common to all divisions, which equals to the case of beta factor $\beta = 1$. For each SW basic event, the CCF between RPS subsystems has been modelled with beta factor $\beta = 0.0280$ (which is α_2 in Appendix 1 of [3]). This means that e.g. PM AS fails in each division of RPS-A with probability 1E-4, and PM AS fails in each division of both RPS-A and RPS-B with probability 2.80E-06. OS basic events of the four AI modules (two in RPS-A and two in RPS-B) have been included in an alpha factor group. Again, the parameters are taken from the model description [3].

It can be noticed that RPS-A and RPS-B are dependent via the PTUs and WDTs. Failures of the PTUs and WDTs were modelled explicitly in an alternative version of the model, but the core damage frequency related to scenarios where PTU or WDT failure contributes to the failure of both subsystems was smaller than 1E-11/year. So it was concluded that PTU and WDT failures do not need to be modelled explicitly.

6. Fault trees

The model employs small fault trees as building blocks. The fault trees related to the EFW are gone through in this section. Other safety functions have been modelled in a similar manner.

EFW system fault tree (Figure 5) contains actuators and links to the dependent systems. RS1 is a link to RS1 signal fault tree. ESF1 signal is assumed to fail if RS1 signal fails and is not modelled separately.

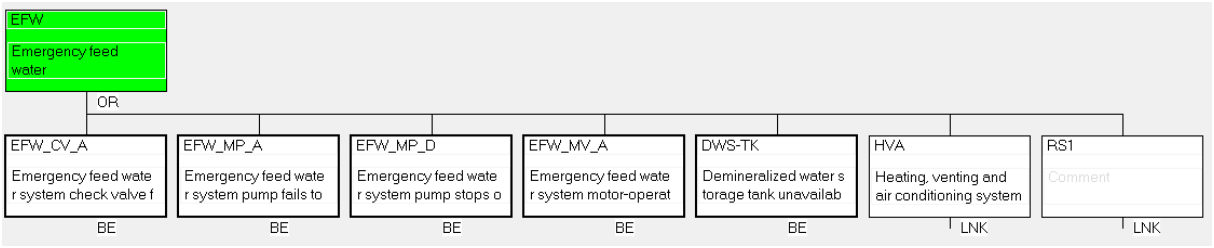


Figure 5: Fault tree of the emergency feed-water system.

RS1 fault tree (Figure 6) contains signals coming from different divisions under an AND gate.

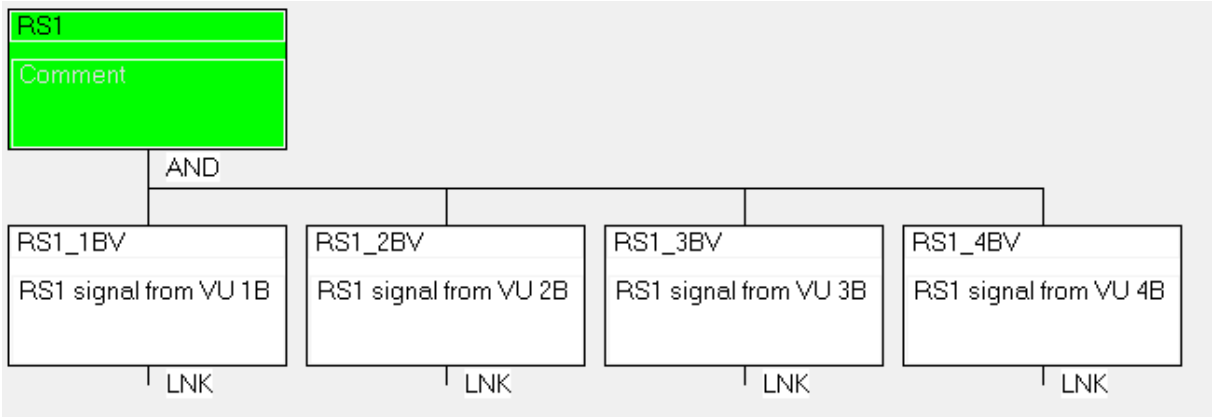


Figure 6: Fault tree of RS1 signal.

VU fault tree for RS1 (Figure 7) contains links to fault trees representing VU modules and the voting logic. Degraded voting logic has been modelled. Three undetected failures of inputs cause the failure of the output. In addition, a combination of two undetected and two detected failures of inputs cause the failure of the output if they are in different divisions. According to the voting logic, three detected failures cause the actuation of the safety function, i.e. prevent the failure. The logic of this fault tree enables CCFs of three and four detected failures to appear in minimal cut sets, but such minimal cut sets are prevented by setting α_3 and α_4 parameters to 0.

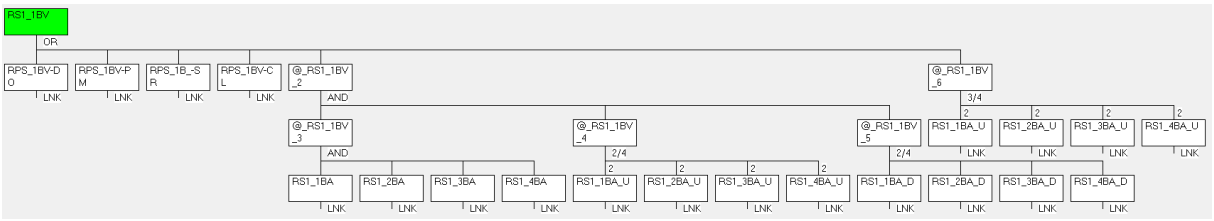


Figure 7: Fault tree of the voting unit in division 1 of RPS-B for RS1 signal.

VU DO fault tree (Figure 8) contains all basic events related to the digital output module. The DO module can fail due to undetected or detected HW failure, or OS failure. It is assumed that a detected failure does not cause the actuation of the safety function, i.e. a detected failure in a VU has similar effect as an undetected failure. It is however assumed that three detected failures in redundant VUs cause the actuation and prevent the failure of the safety function. This is modelled by setting α_3 and α_4 CCF parameters to 0. The results will contain minimal cut sets with e.g. CCF of two modules and one independent detected failure, but such minimal cut sets have very small frequencies, and their existence only causes slight overestimation of the core damage frequency if anything.

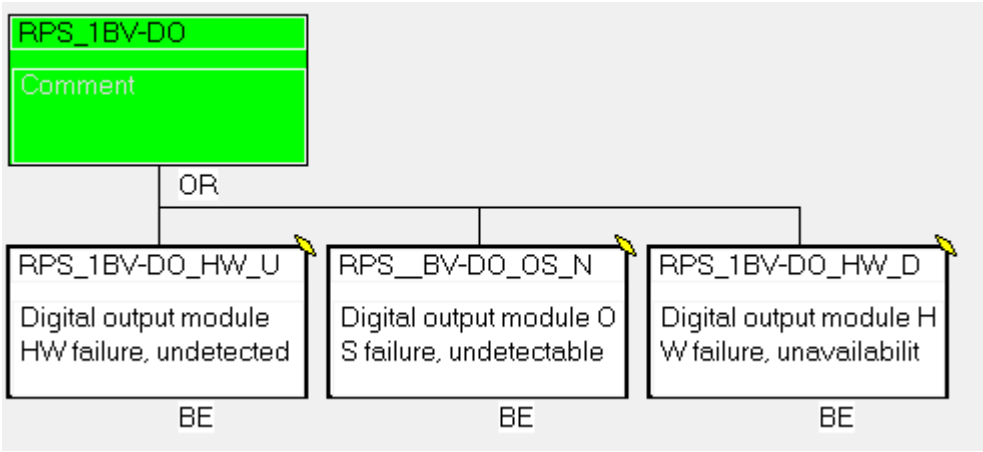


Figure 8: Fault tree of the digital output module in division 1 of RPS-B.

VU PM fault tree (Figure 9) contains all basic events related to the processor module. The PM module can fail due to undetected or detected HW failure, OS failure or AS failure. It is assumed that a detected failure does not cause the actuation of the safety function, i.e. a detected failure in a VU has similar effect as an undetected failure.

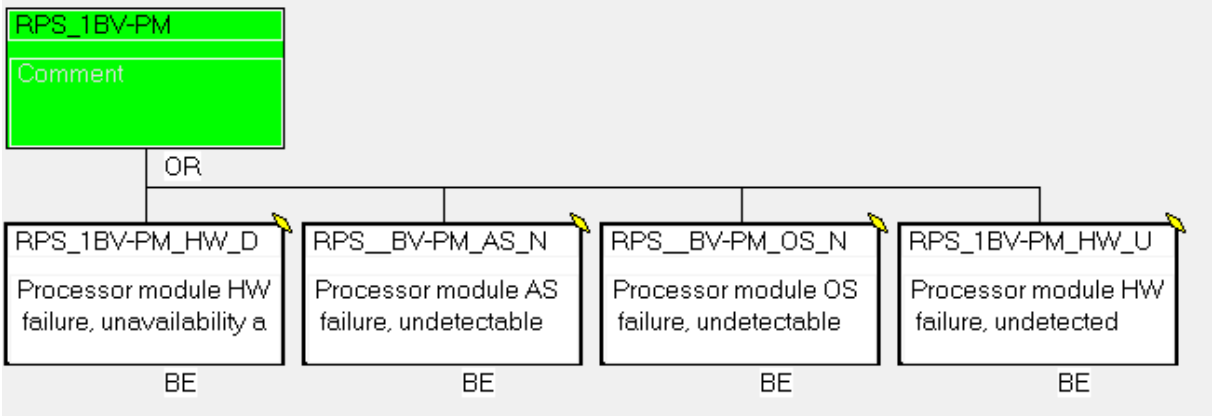


Figure 9: Fault tree of the processor module in the voting unit of division 1 of RPS-B.

SR fault tree (Figure 10) contains links to fault trees representing detected and undetected failures of the sub-rack.

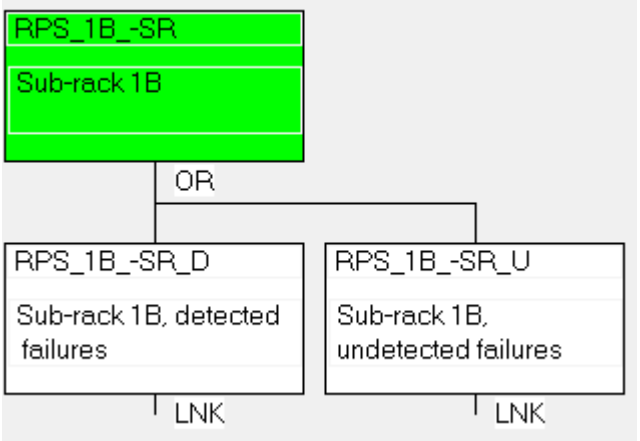


Figure 10: Fault tree of the sub-rack in division 1 of RPS-B.

SR undetected fault tree (Figure 11) contains basic events representing undetected HW failure and OS failure of the sub-rack.

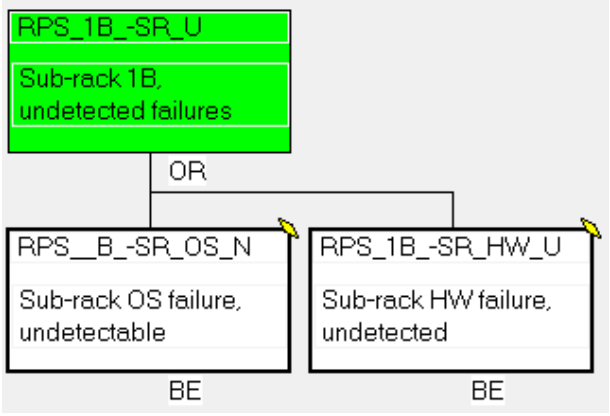


Figure 11: Fault tree of undetected failures of the sub-rack in division 1 of RPS-B.

SR detected fault tree (Figure 12) contains a basic event representing detected HW failure of the sub-rack.

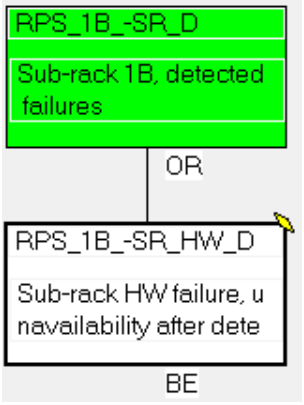


Figure 12: Fault tree of detected failure of the sub-rack in division 1 of RPS-B.

VU CL fault tree (Figure 13) contains all basic events related to the communication link module. The CL module can fail due to undetected or detected HW failure, or OS failure. It is assumed that a detected failure does not cause the actuation of the safety function, i.e. a detected failure in a VU has similar effect as an undetected failure.

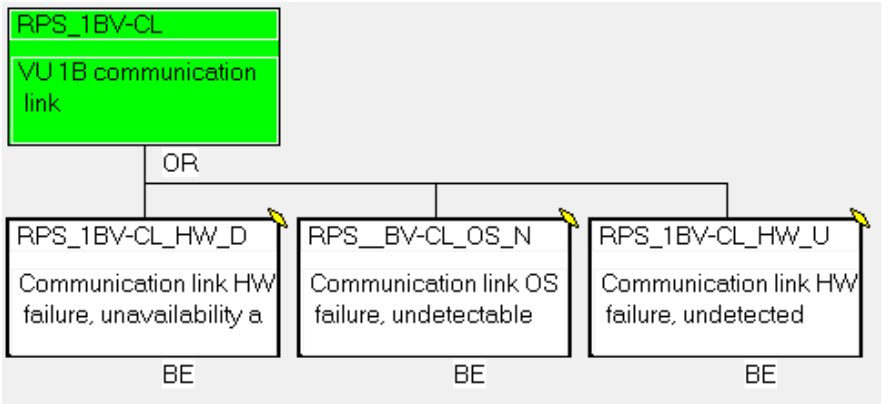


Figure 13: Fault tree of the communication link module in the voting unit of division 1 of RPS-B.

APU fault tree for RS1 (Figure 14) contains links to fault trees containing detected and undetected APU failures. Detected and undetected failures are separated because detected failures change the voting logic (see Figure 7 for the modelling of degraded voting logic).

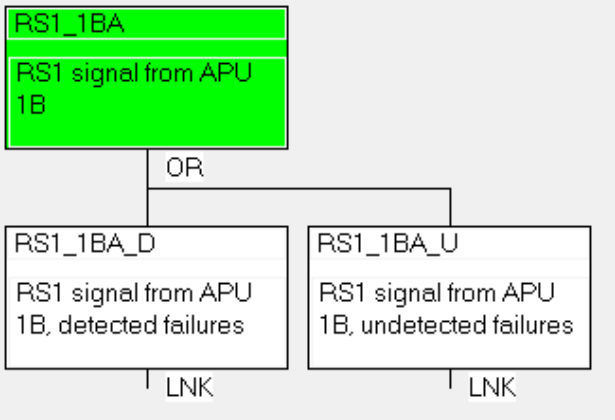


Figure 14: Fault tree of RS1 signal from the APU in division 1 of RPS-B.

APU undetected fault tree for RS1 (Figure 15) contains all undetected APU failures in linked fault trees as well as undetected measurement sensor failure and link to the fault tree of undetected sub-rack failures.

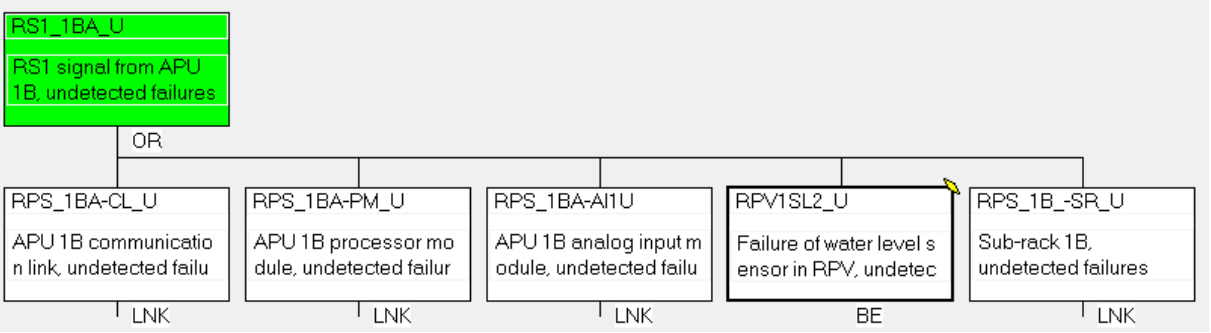


Figure 15: Fault tree of undetected failures related to RS1 signal from the APU in division 1 of RPS-B.

APU CL undetected fault tree (Figure 16) contains basic events representing undetected failures of the communication link module.

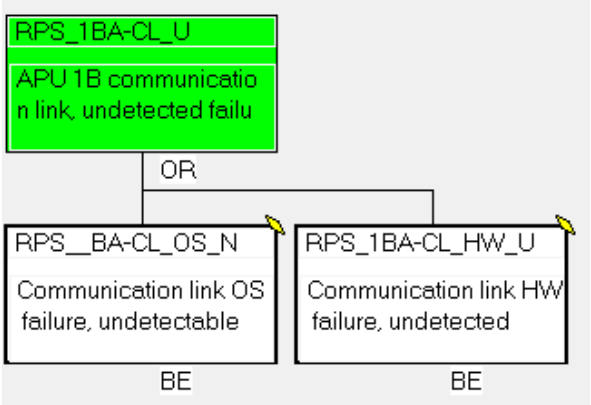


Figure 16: Fault tree of undetected failures of the communication link module in the APU of division 1 of RPS-B.

APU PM undetected fault tree (Figure 17) contains basic events representing undetected failures of the processor module.

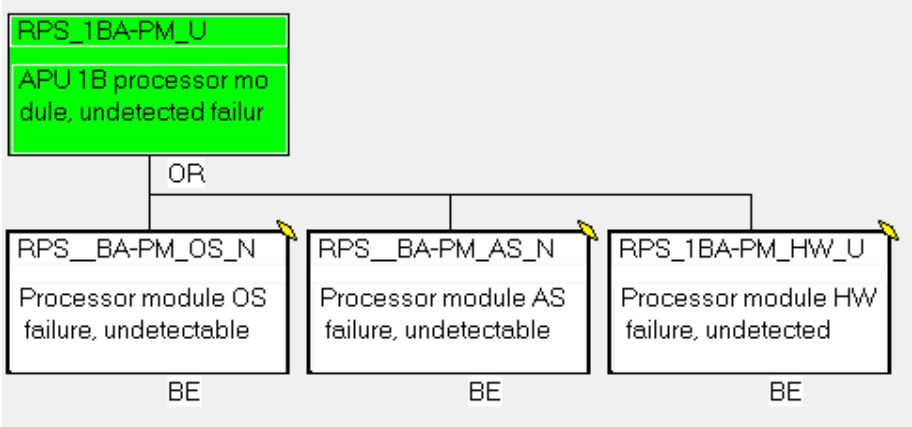


Figure 17: Fault tree of undetected failures of the processor module in the APU of division 1 of RPS-B.

AI undetected fault tree (Figure 18) contains basic events representing undetected failures of the analog input module.

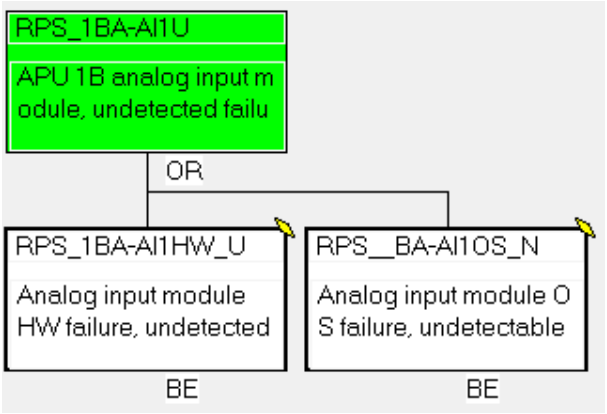


Figure 18: Fault tree of undetected failures of the first analog input module in division 1 of RPS-B.

APU detected fault tree for RS1 (Figure 19) contains all detected APU failures in linked fault trees as well as detected measurement sensor failure and link to the fault tree of detected sub-rack failure.

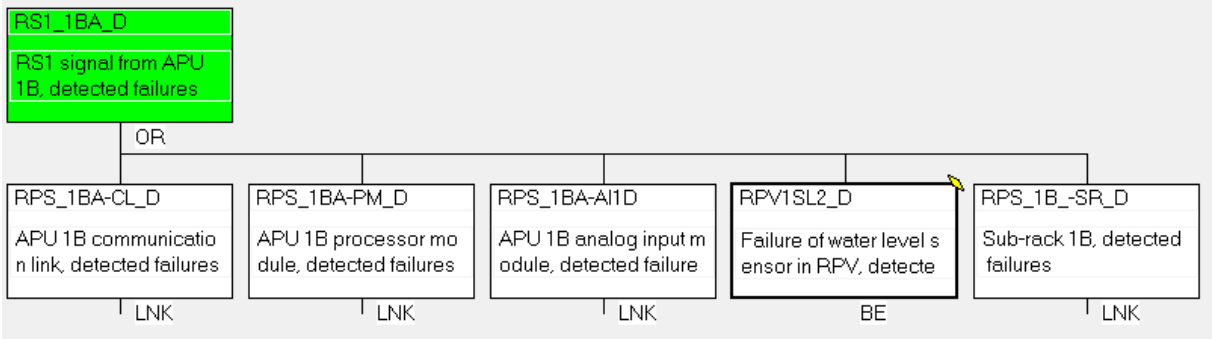


Figure 19: Fault tree of detected failures related to RS1 signal from the APU in division 1 of RPS-B.

APU CL detected fault tree (Figure 20) contains a basic event representing detected failure of the communication link module.

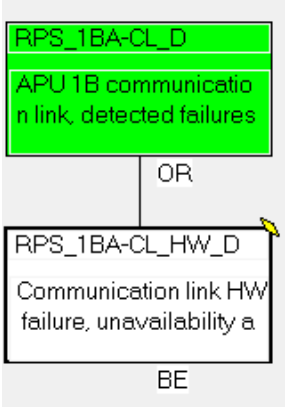


Figure 20: Fault tree of detected failure of the communication link module in the APU of division 1 of RPS-B.

APU PM detected fault tree (Figure 21) contains a basic event representing detected failure of the processor module.

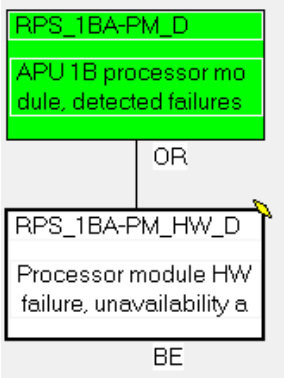


Figure 21: Fault tree of detected failures of the processor module in the APU of division 1 of RPS-B.

AI detected fault tree (Figure 22) contains a basic event representing detected failure of the analog input module.

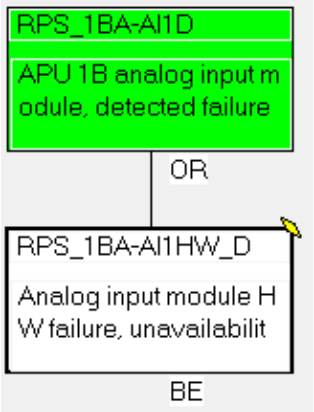


Figure 22: Fault tree of detected failure of the first analog input module in division 1 of RPS-B.

It may seem unnecessary to have fault trees with only one detected failure basic event. The basic events representing detected failures could be moved one fault tree level up. However, if detected failures of OS and AS were modelled, the current structure would clearer. It is also good to treat undetected and detected failures consistently so that they appear at the same fault tree level.

7. Results

7.1 Main results

The core damage frequency is 5.10E-3/year. RPS failures have a quite small contribution to the core damage frequency (Fussell-Vesely 8.51E-4), because safety systems do not contain any redundancy, whereas the RPS does, and because of the 1-out-of-4 actuation criterion of the RPS.

The most important RPS related minimal cut sets are the following:

MCA	5.10E-03	S1-sum	5.22E-03	
Num	Freq.	Prob	Name	Comment
1	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		1.00E-04	RPS__AA-PM_AS_N	Processor module AS failure, undetectable
2	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		1.00E-04	RPS__AV-PM_AS_N	Processor module AS failure, undetectable
3	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		1.00E-04	RPS__BV-PM_AS_N	Processor module AS failure, undetectable
4	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		1.00E-04	RPS__BV-PM_AS_N	Processor module AS failure, undetectable
5	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		1.00E-04	RPS__BA-PM_AS_N	Processor module AS failure, undetectable
6	2.34E-07	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		1.00E-04	RPS__BA-PM_AS_N	Processor module AS failure, undetectable
7	1.40E-07	5.00E-02	LMFW	Loss of main feed water
		2.80E-06	RPS__V-PM_AS_N-AB	2x CCF Processor modules AS (RPS-A and -B)
8	1.40E-07	5.00E-02	LMFW	Loss of main feed water
		2.80E-06	RPS__A-PM_AS_N-AB	2x CCF Processor modules AS (RPS-A and -B)
9	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.32E-05	RPS_AA-CL_HW_U-BCD	3x CCF Communication links HW, undetected
10	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.32E-05	RPS_AA-CL_HW_U-ABC	3x CCF Communication links HW, undetected
11	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.32E-05	RPS_AA-CL_HW_U-ACD	3x CCF Communication links HW, undetected
12	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.32E-05	RPS_AA-CL_HW_U-ABD	3x CCF Communication links HW, undetected
13	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-BCD	3x CCF Communication links HW, undetected
14	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-BCD	3x CCF Communication links HW, undetected
15	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ACD	3x CCF Communication links HW, undetected
16	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ACD	3x CCF Communication links HW, undetected
17	5.43E-08	5.00E-02	LMFW	Loss of main feed water

		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ABD	3x CCF Communication links HW, undetected
18	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ABD	3x CCF Communication links HW, undetected
19	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ABC	3x CCF Communication links HW, undetected
20	5.43E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.32E-05	RPS_BA-CL_HW_U-ABC	3x CCF Communication links HW, undetected
21	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.15E-05	RPS_AV-CL_HW_U-ABCD	4x CCF Communication links HW, undetected
22	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	EFW_MP_D	Emergency feed water system pump stops operating
		2.15E-05	RPS_AA-CL_HW_U-ABCD	4x CCF Communication links HW, undetected
23	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.15E-05	RPS_BV-CL_HW_U-ABCD	4x CCF Communication links HW, undetected
24	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.15E-05	RPS_BV-CL_HW_U-ABCD	4x CCF Communication links HW, undetected
25	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	ECC_MP_D	Emergency core cooling system pump stops operating
		2.15E-05	RPS_BA-CL_HW_U-ABCD	4x CCF Communication links HW, undetected
26	5.03E-08	5.00E-02	LMFW	Loss of main feed water
		4.69E-02	CCW_MP_D	Component cooling water system pump stops operating
		2.15E-05	RPS_BA-CL_HW_U-ABCD	4x CCF Communication links HW, undetected

The most important RPS basic events according to Fussell-Vesely are the following (basic events of other systems have been removed from the list, including the 20 most important basic events):

	Name	Fuss-Ves	Comment
21	RPS__BV-PM_AS_N	9.88E-05	Processor module AS failure, undetectable
22	RPS__BA-PM_AS_N	9.88E-05	Processor module AS failure, undetectable
25	RPS__AV-PM_AS_N	5.30E-05	Processor module AS failure, undetectable
26	RPS__AA-PM_AS_N	5.30E-05	Processor module AS failure, undetectable
28	RPS__V-PM_AS_N-AB	2.75E-05	2x CCF Processor modules AS (RPS-A and -B)
29	RPS__A-PM_AS_N-AB	2.75E-05	2x CCF Processor modules AS (RPS-A and -B)
30	RPS_BA-CL_HW_U-ABD	2.29E-05	3x CCF Communication links HW, undetected
31	RPS_BA-CL_HW_U-ACD	2.29E-05	3x CCF Communication links HW, undetected
32	RPS_BA-CL_HW_U-BCD	2.29E-05	3x CCF Communication links HW, undetected
33	RPS_BA-CL_HW_U-ABC	2.29E-05	3x CCF Communication links HW, undetected
34	RPS_BA-CL_HW_U-ABCD	2.12E-05	4x CCF Communication links HW, undetected
35	RPS_BV-CL_HW_U-ABCD	2.12E-05	4x CCF Communication links HW, undetected
36	RPS_AA-CL_HW_U-ABD	1.23E-05	3x CCF Communication links HW, undetected
37	RPS_AA-CL_HW_U-ACD	1.23E-05	3x CCF Communication links HW, undetected
38	RPS_AA-CL_HW_U-BCD	1.23E-05	3x CCF Communication links HW, undetected
39	RPS_AA-CL_HW_U-ABC	1.23E-05	3x CCF Communication links HW, undetected
40	RPS_AA-CL_HW_U-ABCD	1.14E-05	4x CCF Communication links HW, undetected
41	RPS_AV-CL_HW_U-ABCD	1.14E-05	4x CCF Communication links HW, undetected
42	RPS__BA-AI1OS_N	9.88E-06	Analog input module OS failure, undetectable
43	RPS__BA-CL_OS_N	9.88E-06	Communication link OS failure, undetectable
44	RPS__BA-PM_OS_N	9.88E-06	Processor module OS failure, undetectable
45	RPS__BV-DO_OS_N	9.88E-06	Digital output module OS failure, undetectable
46	RPS__BV-PM_OS_N	9.88E-06	Processor module OS failure, undetectable
47	RPS__B_-SR_OS_N	9.88E-06	Sub-rack OS failure, undetectable
48	RPS__BV-CL_OS_N	9.88E-06	Communication link OS failure, undetectable
49	RPS_BA-AI1HW_U-ABD	8.86E-06	3x CCF Analog input modules HW, undetected
50	RPS_BA-AI1HW_U-ACD	8.86E-06	3x CCF Analog input modules HW, undetected
51	RPS_BA-AI1HW_U-BCD	8.86E-06	3x CCF Analog input modules HW, undetected
52	RPS_BA-AI1HW_U-ABC	8.86E-06	3x CCF Analog input modules HW, undetected
53	RPS_BV-DO_HW_U-ABCD	8.49E-06	4x CCF Digital output modules HW, undetected
54	RPS_BA-AI1HW_U-ABCD	8.20E-06	4x CCF Analog input modules HW, undetected
55	RPS__AA-PM_OS_N	5.30E-06	Processor module OS failure, undetectable
56	RPS__AA-CL_OS_N	5.30E-06	Communication link OS failure, undetectable
57	RPS__AV-CL_OS_N	5.30E-06	Communication link OS failure, undetectable
58	RPS__A_-SR_OS_N	5.30E-06	Sub-rack OS failure, undetectable
59	RPS__AV-PM_OS_N	5.30E-06	Processor module OS failure, undetectable
60	RPS__AV-DO_OS_N	5.30E-06	Digital output module OS failure, undetectable
61	RPS__AA-AI2OS_N	5.29E-06	Analog input module OS failure, undetectable
62	RPS__AA-AI1OS_N	5.28E-06	Analog input module OS failure, undetectable
63	RPS_AA-AI2HW_U-ABD	4.74E-06	3x CCF Analog input modules HW, undetected

64	RPS_AA-AI2HW_U-ACD	4.74E-06	3x CCF Analog input modules HW, undetected
65	RPS_AA-AI2HW_U-BCD	4.74E-06	3x CCF Analog input modules HW, undetected
66	RPS_AA-AI2HW_U-ABC	4.74E-06	3x CCF Analog input modules HW, undetected
67	RPS_AA-AI1HW_U-ABD	4.73E-06	3x CCF Analog input modules HW, undetected
68	RPS_AA-AI1HW_U-ACD	4.73E-06	3x CCF Analog input modules HW, undetected
69	RPS_AA-AI1HW_U-BCD	4.73E-06	3x CCF Analog input modules HW, undetected
70	RPS_AA-AI1HW_U-ABC	4.73E-06	3x CCF Analog input modules HW, undetected
71	RPS_AV-DO_HW_U-ABCD	4.56E-06	4x CCF Digital output modules HW, undetected
72	RPS_BA-PM_HW_U-ABC	4.52E-06	3x CCF Processor modules HW, undetected
73	RPS_BA-PM_HW_U-BCD	4.52E-06	3x CCF Processor modules HW, undetected
74	RPS_BA-PM_HW_U-ACD	4.52E-06	3x CCF Processor modules HW, undetected
75	RPS_BA-PM_HW_U-ABD	4.52E-06	3x CCF Processor modules HW, undetected
76	RPS_AA-AI2HW_U-ABCD	4.39E-06	4x CCF Analog input modules HW, undetected
77	RPS_AA-AI1HW_U-ABCD	4.38E-06	4x CCF Analog input modules HW, undetected
82	RPS_BA-PM_HW_U-ABCD	4.18E-06	4x CCF Processor modules HW, undetected
83	RPS_BV-PM_HW_U-ABCD	4.12E-06	4x CCF Processor modules HW, undetected
85	RPS__A-CL_OS_N-AB	2.75E-06	2x CCF Communication links OS (RPS-A and -B)
86	RPS__A-PM_OS_N-AB	2.75E-06	2x CCF Processor modules OS (RPS-A and -B)
87	RPS__V-DO_OS_N-AB	2.75E-06	2x CCF Digital output modules OS (RPS-A and -B)
88	RPS__V-PM_OS_N-AB	2.75E-06	2x CCF Processor modules OS (RPS-A and -B)
89	RPS___-SR_OS_N-AB	2.75E-06	2x CCF Sub-rack OS (RPS-A and -B)
90	RPS__V-CL_OS_N-AB	2.75E-06	2x CCF Communication links OS (RPS-A and -B)
91	RPS_AA-PM_HW_U-ABC	2.43E-06	3x CCF Processor modules HW, undetected
92	RPS_AA-PM_HW_U-BCD	2.43E-06	3x CCF Processor modules HW, undetected
93	RPS_AA-PM_HW_U-ACD	2.43E-06	3x CCF Processor modules HW, undetected
94	RPS_AA-PM_HW_U-ABD	2.43E-06	3x CCF Processor modules HW, undetected
99	RPS__A-AI_OS_N-AB	2.31E-06	2x CCF AI1 OS in RPS-A and -B
100	RPS__A-AI_OS_N-BC	2.31E-06	2x CCF AI2 OS in RPS-A and AI1 OS in RPS-B
101	RPS_AA-PM_HW_U-ABCD	2.25E-06	4x CCF Processor modules HW, undetected
102	RPS_AV-PM_HW_U-ABCD	2.21E-06	4x CCF Processor modules HW, undetected
104	RPS__A-AI_OS_N-AD	2.12E-06	2x CCF AI1 OS in RPS-A and AI2 OS in RPS-B

The most important RPS basic events according to the risk increase factor are the following (basic events of other systems have been removed from the list):

	Name	Risk incr.	Comment
2	RPS__A-CL_OS_N-AB	1.08E+01	2x CCF Communication links OS (RPS-A and -B)
3	RPS__A-PM_OS_N-AB	1.08E+01	2x CCF Processor modules OS (RPS-A and -B)
4	RPS__A-PM_AS_N-AB	1.08E+01	2x CCF Processor modules AS (RPS-A and -B)
5	RPS__A-AI_OS_N-AB	1.08E+01	2x CCF AI1 OS in RPS-A and -B
6	RPS__V-DO_OS_N-AB	1.08E+01	2x CCF Digital output modules OS (RPS-A and -B)
7	RPS__V-PM_AS_N-AB	1.08E+01	2x CCF Processor modules AS (RPS-A and -B)
8	RPS__V-PM_OS_N-AB	1.08E+01	2x CCF Processor modules OS (RPS-A and -B)
9	RPS___-SR_OS_N-AB	1.08E+01	2x CCF Sub-rack OS (RPS-A and -B)
10	RPS__V-CL_OS_N-AB	1.08E+01	2x CCF Communication links OS (RPS-A and -B)
11	RPS__A-AI_OS_N-BC	1.08E+01	2x CCF AI2 OS in RPS-A and AI1 OS in RPS-B
20	RPS__A-AI_OS_N-AD	9.86E+00	2x CCF AI1 OS in RPS-A and AI2 OS in RPS-B
21	RPS_BA-AI1HW_U-ABCD	1.99E+00	4x CCF Analog input modules HW, undetected
23	RPS__BA-AI1OS_N	1.99E+00	Analog input module OS failure, undetectable
24	RPS_BA-AI1HW_U-ABD	1.99E+00	3x CCF Analog input modules HW, undetected
26	RPS_BA-AI1HW_U-ACD	1.99E+00	3x CCF Analog input modules HW, undetected
28	RPS_BA-AI1HW_U-BCD	1.99E+00	3x CCF Analog input modules HW, undetected
30	RPS_BA-AI1HW_U-ABC	1.99E+00	3x CCF Analog input modules HW, undetected
32	RPS_B_-SR_HW_U-ABC	1.99E+00	3x CCF Sub-racks HW, undetected
33	RPS_B_-SR_HW_U-BCD	1.99E+00	3x CCF Sub-racks HW, undetected
34	RPS_B_-SR_HW_U-ACD	1.99E+00	3x CCF Sub-racks HW, undetected
35	RPS_B_-SR_HW_U-ABD	1.99E+00	3x CCF Sub-racks HW, undetected
36	RPS__B_-SR_OS_N	1.99E+00	Sub-rack OS failure, undetectable
37	RPS_B_-SR_HW_U-ABCD	1.99E+00	4x CCF Sub-racks HW, undetected
38	RPS_BA-PM_HW_U-ABC	1.99E+00	3x CCF Processor modules HW, undetected
39	RPS_BA-CL_HW_U-ABC	1.99E+00	3x CCF Communication links HW, undetected
40	RPS_BA-PM_HW_U-BCD	1.99E+00	3x CCF Processor modules HW, undetected
41	RPS_BA-CL_HW_U-BCD	1.99E+00	3x CCF Communication links HW, undetected
42	RPS_BA-PM_HW_U-ACD	1.99E+00	3x CCF Processor modules HW, undetected
43	RPS_BA-CL_HW_U-ACD	1.99E+00	3x CCF Communication links HW, undetected
44	RPS_BA-PM_HW_U-ABD	1.99E+00	3x CCF Processor modules HW, undetected
45	RPS_BA-CL_HW_U-ABD	1.99E+00	3x CCF Communication links HW, undetected
46	RPS__BA-CL_OS_N	1.99E+00	Communication link OS failure, undetectable
47	RPS__BA-PM_OS_N	1.99E+00	Processor module OS failure, undetectable
48	RPS__BA-PM_AS_N	1.99E+00	Processor module AS failure, undetectable
49	RPS_BA-PM_HW_U-ABCD	1.99E+00	4x CCF Processor modules HW, undetected
50	RPS_BA-CL_HW_U-ABCD	1.99E+00	4x CCF Communication links HW, undetected
51	RPS__BV-DO_OS_N	1.99E+00	Digital output module OS failure, undetectable
52	RPS__BV-PM_AS_N	1.99E+00	Processor module AS failure, undetectable
53	RPS__BV-PM_OS_N	1.99E+00	Processor module OS failure, undetectable

54	RPS__BV-CL_OS_N	1.99E+00	Communication link OS failure, undetectable
55	RPS_BV-CL_HW_U-ABCD	1.99E+00	4x CCF Communication links HW, undetected
56	RPS_BV-PM_HW_U-ABCD	1.99E+00	4x CCF Processor modules HW, undetected
57	RPS_BV-DO_HW_U-ABCD	1.99E+00	4x CCF Digital output modules HW, undetected
58	RPS__A-AI_OS_N-BD	1.96E+00	2x CCF Analog input modules OS (RPS-B)
66	RPS_A_-SR_HW_U-ABD	1.53E+00	3x CCF Sub-racks HW, undetected
67	RPS_A_-SR_HW_U-ACD	1.53E+00	3x CCF Sub-racks HW, undetected
68	RPS_A_-SR_HW_U-BCD	1.53E+00	3x CCF Sub-racks HW, undetected
69	RPS_A_-SR_HW_U-ABC	1.53E+00	3x CCF Sub-racks HW, undetected
70	RPS__AV-DO_OS_N	1.53E+00	Digital output module OS failure, undetectable
71	RPS__AV-PM_AS_N	1.53E+00	Processor module AS failure, undetectable
72	RPS__AV-PM_OS_N	1.53E+00	Processor module OS failure, undetectable
73	RPS__AV-CL_OS_N	1.53E+00	Communication link OS failure, undetectable
74	RPS_AV-CL_HW_U-ABCD	1.53E+00	4x CCF Communication links HW, undetected
75	RPS_AV-PM_HW_U-ABCD	1.53E+00	4x CCF Processor modules HW, undetected
76	RPS_AV-DO_HW_U-ABCD	1.53E+00	4x CCF Digital output modules HW, undetected
77	RPS__AA-CL_OS_N	1.53E+00	Communication link OS failure, undetectable
78	RPS__AA-PM_OS_N	1.53E+00	Processor module OS failure, undetectable
79	RPS__AA-PM_AS_N	1.53E+00	Processor module AS failure, undetectable
80	RPS_AA-PM_HW_U-ABCD	1.53E+00	4x CCF Processor modules HW, undetected
81	RPS_AA-CL_HW_U-ABCD	1.53E+00	4x CCF Communication links HW, undetected
82	RPS_AA-PM_HW_U-ABD	1.53E+00	3x CCF Processor modules HW, undetected
83	RPS_AA-CL_HW_U-ABD	1.53E+00	3x CCF Communication links HW, undetected
84	RPS_AA-PM_HW_U-ACD	1.53E+00	3x CCF Processor modules HW, undetected
85	RPS_AA-CL_HW_U-ACD	1.53E+00	3x CCF Communication links HW, undetected
86	RPS_AA-PM_HW_U-BCD	1.53E+00	3x CCF Processor modules HW, undetected
87	RPS_AA-CL_HW_U-BCD	1.53E+00	3x CCF Communication links HW, undetected
88	RPS_AA-PM_HW_U-ABC	1.53E+00	3x CCF Processor modules HW, undetected
89	RPS_AA-CL_HW_U-ABC	1.53E+00	3x CCF Communication links HW, undetected
90	RPS__A_-SR_OS_N	1.53E+00	Sub-rack OS failure, undetectable
91	RPS_A_-SR_HW_U-ABCD	1.53E+00	4x CCF Sub-racks HW, undetected
93	RPS__AA-AI2OS_N	1.53E+00	Analog input module OS failure, undetectable
95	RPS_AA-AI2HW_U-ABCD	1.53E+00	4x CCF Analog input modules HW, undetected
97	RPS_AA-AI2HW_U-ABD	1.53E+00	3x CCF Analog input modules HW, undetected
99	RPS_AA-AI2HW_U-ACD	1.53E+00	3x CCF Analog input modules HW, undetected
101	RPS_AA-AI2HW_U-BCD	1.53E+00	3x CCF Analog input modules HW, undetected
103	RPS_AA-AI2HW_U-ABC	1.53E+00	3x CCF Analog input modules HW, undetected
104	RPS_AA-AI1HW_U-ABCD	1.53E+00	4x CCF Analog input modules HW, undetected
105	RPS__AA-AI1OS_N	1.53E+00	Analog input module OS failure, undetectable
106	RPS_AA-AI1HW_U-ABD	1.53E+00	3x CCF Analog input modules HW, undetected
107	RPS_AA-AI1HW_U-ACD	1.53E+00	3x CCF Analog input modules HW, undetected
108	RPS_AA-AI1HW_U-BCD	1.53E+00	3x CCF Analog input modules HW, undetected
109	RPS_AA-AI1HW_U-ABC	1.53E+00	3x CCF Analog input modules HW, undetected

Table 5 presents total Fussell-Vesely values of HW, AS and OS failures. Total Fussell-Vesely values of the sensor types are also presented. The sensors are not counted as RPS components.

Table 5: Fussell-Vesely values of HW, AS and OS failures.

Component type	Fussell-Vesely	Portion of the RPS related risk
Hardware	3.60E-4	42.3%
Application software	3.58E-4	42.1%
Operating system	1.35E-4	15.9%
Water level sensors	3.36E-5	-
Pressure sensors	1.23E-5	-
Temperature sensors	1.50E-7	-

7.2 Detected failures

The total Fussell-Vesely of detected failures is smaller than 1E-7, so small that different quantification algorithms give very different values. Reasons for the small contribution are the small probabilities of detected failures and the voting logic, which works so that three detected failures cause actuation of a safety function. Furthermore, software failures were assumed to be never detected, and spurious actuations were not included in the model. In [6], the contribution of detected failures was found high due to spurious actuations. But with the specifications given in [3], detected failures could have been left out of the model, and the results would not have changed significantly.

An alternative model version with different voting logic was implemented. In this version, the voting logic is 1-out-of-1 after three detected failures, and four detected failures prevent the actuation of the safety function. RPS failures have slightly higher contribution to the total frequency (Fussell-Vesely 8.54E-4). The addition to the RPS contribution comes from detected failures, but still the contribution of detected failures is quite small (Fussell-Vesely 2.72E-6, portion of the RPS related risk 0.32%). Obviously, the contribution would increase more if detected software failures were modelled, the failure rates of RPS modules were increased, the mean time to repair was increased or CCF parameters were increased. It is theoretically possible that detected failures could contribute significantly to the core damage risk.

It can be questioned if it is worthwhile to model detected failures at all when modelling failures of start/open signals. Undetected and detected failures could be merged together and treated conservatively as undetected. It would simplify fault trees, because there would not be need to model degraded voting logic. However, detected failures could become more significant if spurious actuations were analysed.

7.3 Software failures

Significant portion of the contribution of the RPS to core damage risk comes from application software failures due to high probabilities and the assumption of beta factor $\beta = 1$ for the CCF between divisions. The CCF of AS modules between subsystems has a significant contribution, because it can cause diverse safety functions to fail and alone cause the core damage after the initiating event.

The AS failure probabilities used in the study are quite large compared to probabilities used in some other studies, such as [6]. If AS failure probabilities are decreased to 1E-5, Fussell-Vesely of the RPS is decreased to 5.29E-4, which means that the relative decrease is 38%. The total Fussell-Vesely of AS failures is 3.58E-5, which is 10% of the nominal value in Table 5.

A different way of modelling application software was tested with an alternative model version. In this version, separate AS basic events were used for different signals (e.g. separate basic events of APU PM AS for RS2, ESF3 and ESF2). CCF between different AS in the same module was modelled with beta factor 0.028. With this change, Fussell-Vesely of the RPS decreased to 7.01E-4, which means that the relative decrease was 18%. The total Fussell-Vesely of AS failures was 2.08E-4. The reason for the decrease was that e.g. minimal cut sets 3-8 listed in the beginning of Section 7.1 had much smaller probabilities, and that failure of processing an individual signal cannot cause the EFW to fail, whereas failure of all AS in the PM can. The contribution decreased even though the total AS failure probability increased, because there were more AS basic events with probability 1E-4.

Furthermore, the above described model version was modified so that the probabilities of the AS basic events were divided by three, because three different signals are processed in each PM. This way the total AS failure probability of a PM was 1E-4. Fussell-Vesely of the RPS

decreased to 5.62E-4, and the relative decrease was thus 34%. The total Fussell-Vesely of AS failures was 6.90E-5.

The analyses described above are summarised in Table 6.

Table 6: Application software analysis cases.

Analysis case	**Fussell-Vesely of RPS**	**Relative decrease of RPS FV**	**Fussell-Vesely of AS failures**
AS failure probabilities decreased to 1E-5	5.29E-4	38%	3.58E-5
Separate AS basic events for different signals, probabilities 1E-4	7.01E-4	18%	2.08E-4
Separate AS basic events for different signals, probabilities 3.33E-5	5.62E-4	34%	6.90E-5

When AS failure probabilities are this high, the selection of basic events can affect the results significantly. The contents of the AS were not specified for the study. In reality, AS function block diagrams should be analysed when selecting the basic events and the probabilities.

7.4 Fault tolerant techniques

Table 7 presents the sensitivity studies performed on fault tolerant techniques. The analyses were performed by recalculating the probabilities of undetected HW failures under different assumptions. The recalculations were performed using the supporting fault trees discussed in Section 5.1, and the new probabilities were then imported to the main model in each analysis case. The testing intervals of measurement sensors were also changed in the analysis cases concerning full-scope testing. The contribution of the RPS to the total risk is studied in each analysis case. Table 7 presents also the ratio between the RPS Fussell-Vesely of the analysis case and the baseline RPS Fussell-Vesely (8.51E-4), which is calculated by dividing the RPS Fussell-Vesely of the analysis case by the baseline value.

The sensitivity studies show that without automatic and periodic testing the RPS related risk increases over 270%. Periodic testing is found more important than automatic testing, because communication link failures are not detected by automatic testing and the communication links are the most important RPS modules with regard to HW as can be seen in the main results of Section 7.1. Most of the unavailability related to RPS HW comes from failures that are not detected by automatic testing nor periodic testing. By increasing the coverage of automatic or periodic testing, significant improvements could by achieved. If automatic testing or periodic testing were able to detect all HW failures, the risk related to RPS HW would be insignificant, and SW failures would dominate the RPS risk. The RPS related risk can also be significantly decreased by performing full-scope tests more often. The RPS related risk is not very sensitive with regard to the periodic testing interval. Even if periodic testing is performed only once a week, the risk does not increase much.

Table 7: Sensitivity analyses for fault tolerant techniques.

Analysis case	Fussell-Vesely of RPS	Ratio compared to baseline RPS Fussell-Vesely
Automatic testing always detects all HW failures	4.92E-4	57.8%
Automatic testing fails completely	1.70E-3	200%
Periodic testing always detects all HW failures not detected by automatic testing	4.99E-4	58.6%
Periodic testing fails completely (PTU fails)	1.97E-3	231%
Automatic testing and periodic testing fail completely	3.16E-3	371%
Full-scope testing is performed every 3 months	6.70E-4	78.7%
Full-scope testing is performed every 12 months	1.24E-3	146%
Periodic testing is performed every week	8.86E-4	104%
Fault tolerant techniques do not fail	8.43E-4	99.1%

With assumption that fault tolerant techniques (PTU, WDT and automatic testing in processor modules) never fail, the contribution of RPS decreased less than 1%. This result can be considered a lower bound with regard to the probabilities of undetected HW failures, whereas the main model provided an upper bound. In Section 5.1, the probabilities were estimated conservatively for the main model. Since the lower bound and upper bound are so close to each other, it can be concluded that the conservative formula used in Section 5.1 is sufficient, and the results would not change significantly if the probabilities were estimated more accurately with regard to scenarios where fault tolerant techniques fail.

8. Conclusions

This report presented a PRA model of a fictive and simplified BWR plant focusing on digital I&C. The model will be used in the international benchmark study organized by WGRISK project DIGMAP. The selected modelling approach is close to the previous model of the DIGREL project [6] employing small fault trees as building blocks. I&C component failures have been divided into detected failures and undetected failures. Significant portion of the contribution of the RPS related risk comes from application software failures, along with undetected hardware failures. On the other hand, detected hardware failures in the RPS have insignificant contribution to the core damage risk, likely because spurious actuations have not been analysed. The importance of automatic testing and periodic testing as fault tolerant techniques to reduce the risk of undetected hardware failures was recognized in the sensitivity studies. Selection of common cause failure groups and parameters, and application software basic events are expected to be major issues in the benchmark study.

References

[1] Nuclear Energy Agency. Failure modes taxonomy for reliability assessment of digital instrumentation and control systems for probabilistic risk analysis. OECD NEA/CSNI/R(2014)16, Organization for Economic Co-operation and Development, February 2015.

[2] Porthin, M. Progress of WGRISK digital I&C benchmark study DIGMAP in 2017 (D1.3.2). VTT-R-06873-17, VTT Technical Research Centre of Finland Ltd, Espoo, 2018.

[3] Working group on risk assessment (WGRISK). Description of example plant model for DI&C PSA comparative study. Nuclear Energy Agency, 2018.

[4] Holmberg, J-E. DIGREL example PSA model description. Report 14127_R001, Risk Pilot, 3 March 2016.

[5] Lee, SJ, Jung, W, Yang, J-E. PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems. Annals of Nuclear Energy, 87, 375-384, 2016.

[6] Authen, S, Holmberg, J-E, Tyrväinen, T, Zamani, L. Guidelines for reliability analysis of digital systems in PSA context - Final report. NKS-330, Nordic nuclear safety research (NKS), Roskilde, 2015.